Remarks

Applicant carefully considered the Office Action mailed on March 16, 2005. Claims 1-101 are pending in the present patent application. Of the pending claims, the Examiner rejected claims 1-101. In response to the Office Action, Applicant amended claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101. No new matter has been added. In view of the above amendment and the following remarks, Applicant requests further examination and reconsideration of the present patent application.

The Examiner rejected claims 1-101 under 35 USC §102(e) as being anticipated by Lloyd et al. (US Patent No. 6,219,790). Applicant respectfully traverses the §102(e) rejection of claims 1-101 and submits that Lloyd et al. (hereinafter Lloyd) does not anticipate the claimed invention.

The present invention, as claimed in independent claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101 are patentable over the Lloyd reference. "Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." W.L. Gore & Associates v. Garlock, Inc., 220 USPQ 303, 313 (Fed. Cir. 1983). The Lloyd reference does not disclose each element of the present invention as claimed in independent claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101.

In one form or another, independent claims 1, 10, 27, 54, 62, 92 and 100 of the present invention recite a gateway device for securely managing activities between at least one device and at least one service provider. The gateway device comprises an authenticator that authenticates the identity of the at least one service provider and the at least one device; an access authorizer that permits the at least one service provider to interact with the at least one device; and an activity manager, responsive to the access authorizer and the authenticator, that manages the activities occurring between the at least one service provider and the at least one device, wherein the activities comprise exchanging status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider.

Independent claims 19, 70 and 101 of the present invention, in one form or another, recite a gateway device for securely managing activities between at least one device and at least one service provider. The gateway device comprises a request handler that receives activity requests from the at least one service provider and the at least one device; an authenticator that authenticates the identity of the at least one service provider and the at least one device; an access authorizer that permits the at least one service provider to interact with the at least one device; an activity manager that manages the activity requests occurring between the at least one service provider and the at least one device, wherein the activity requests comprise exchanging status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider; and a response component, responsive to the request handler, the authenticator, the access authorizer and the activity manager, that receives activity responses from the at least one service provider and the at least one device..

Independent claim 26 of the present invention recites a gateway device for securely managing activities between at least one device and at least one service provider. The gateway device comprises a request handler that receives activity requests from the at least one service provider and the at least one device; an authenticator that authenticates the identity of the at least one service provider and the at least one device; an access authorizer that permits the at least one service provider to interact with the at least one device; an activity manager that manages the activity requests occurring between the at least one service provider and the at least one device, wherein the activity requests comprise exchanging status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider; a data format translator that translates the format of data transmitted and received by the at least one service provider and the at least one device during the activities; and a response component, responsive to the request handler, the authenticator, the access authorizer, the activity manager, and the data format translator that receives activity responses from the at least one service provider and the at least one device.

Independent claims 36 and 76 of the present invention, in one form or another, recite a system for securely providing services between a first site and a second site. The system comprises at least one appliance linked in a first network at the first site and a service provider

linked to the at least one appliance in a second network at the second site. The system further comprises a gateway device that securely manages the services provided between the at least one appliance and the service provider. The gateway device comprises an authenticator that authenticates the identity of the service provider and the at least one appliance. The gateway device further comprises an access authorizer that permits the service provider to interact with the at least one appliance, and a service manager, responsive to the authenticator and the access authorizer, that manages the services provided between the service provider and the at least one appliance, wherein the services comprise exchanging status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider.

In addition, independent claims 45 and 84 of the present invention, in one form or another, recite a system for securely providing remote monitoring and diagnostics. The system comprises at least one device linked to a first network and a service provider linked to the at least one device in a second network. The system further comprises a gateway device that securely manages remote monitoring and diagnostic activities between the at least one device and the service provider. The gateway device comprises an authenticator that authenticates the identity of the service provider and the at least one device. The gateway device further comprises an access authorizer that permits the service provider to interact with the at least one device; and an activity manager, responsive to the authenticator and access authorizer, that manage the remote monitoring and diagnostic activities provided between the service provider and the at least one device, wherein the monitoring and diagnostic activities comprise exchanging status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider.

Applicant respectfully submits that the Lloyd reference does not show or disclose each element of the Applicant's recited invention. Lloyd does not disclose a gateway device for securely managing activities between a device and a service provider, wherein the gateway device comprises an authenticator that authenticates the identity of the service provider and the device; an access authorizer that permits the service provider to interact with the device; and an activity manager, responsive to the access authorizer and the authenticator, that manages the activities occurring between the service provider and the device, wherein the activities comprise exchanging status information, diagnostic

information, usage history, notifications of failure and status updates between the device and the service provider.

The Examiner referenced col. 3, lines 23-30, as being relevant to a gateway device including an authenticator that authenticates the identity of a service provider and a device. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a gateway device including an authenticator that authenticates the identity of a service provider and a device. Instead, the material in col. 3, lines 23-30 relates to a mechanism for authenticating and authorizing user access to a computer network by determining if the login information provided by a user matches information stored in a user record.

The Examiner also referenced col. 5, lines 47-51 as being relevant to an authenticator that authenticates the identity of a device. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a device that is authenticated. Instead the material in col. 5, lines 47-51 relates to a Network Server Access (NAS) device that is connected to a user's workstation, wherein the NAS device creates a data packet that forms an authentication request for a user who is requesting access the network. The data packet comprises information identifying the particular NAS sending the authentication request, the port being used for the modem connection and the user name and password provided by the user.

In addition, the Examiner referenced col. 4, lines 15-21, and col. 5, lines 5-16 as being relevant to an authenticator that authenticates the identity of a service provider. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a service provider that is authenticated. Instead, the material in col. 4, lines 15-21, and col. 5, lines 5-16 relates to the types of network elements that are attached to the network, wherein the network elements represent certain services that are available to users having access to the network.

The teaching in these sections is not analogous to the claimed limitation because there is no mention of a gateway device for securely managing activities between a device and a service provider. In the present invention, the gateway device securely manages activities

between a device and a service provider in order to obtain information such as status information, diagnostic information and usage history from the device and offer information to the provider about the device such as notifications of failure and status updates.

Lloyd does not teach these limitations because it is not concerned with a gateway device for securely managing activities between devices and providers, wherein the activities comprise exchanging status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider. Instead, Lloyd is concerned with the creation of a centralized general-purpose authentication authorization and accounting (AAA) server for maintaining accounting information, user authentication information and authorization information for a user who is requesting access to a network.

The Examiner also referenced col. 12, lines 8-15 and col. 11, lines 16-23 as being relevant to a gateway device that includes an access authorizer that permits a service provider to interact with a device. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a gateway device that includes an access authorizer that permits a service provider to interact with a device. Instead the material in col. 12, lines 8-15 and col. 11, lines 16-23 relates to checking the accuracy of a user's login information using a permit, wherein a permit is required to be held by a user who is requesting access to a service, such as a news service, a WWW service and a mail service (see, for e.g., col. 5, lines 5-12 in Lloyd) provided by the network. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device that includes an access authorizer that permits a service provider to interact with a device. Lloyd does not teach this limitation because it is not concerned with a gateway device that includes an access authorizer that permits a service provider to interact with a device.

The Examiner also referenced col. 13 lines 2-21 as being relevant to an activity manager that manages the activities occurring between the service provider and the device. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of an activity manager that manages the activities occurring between the service provider and the device, wherein the activities comprise exchanging

status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider. Instead, this section relates to providing information related to session establishment and termination by clients/users and providing reports to users for billing and statistics gathering purposes. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device that includes an activity manager that manages the activities occurring between the service provider and the device, wherein the activities comprise exchanging status information, diagnostic information, usage history, notifications of failure and status updates between the device and the service provider. Lloyd does not teach this limitation because it is not concerned with a gateway device that includes an activity manager that manages the activities occurring between the service provider and the device.

The Examiner referenced col. 5, lines 59-64 as being relevant to a request handler that receives activity requests from the service provider and the device. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a request handler that receives activity requests from the service provider and the device, wherein the activity requests comprise exchanging status information, diagnostic information, usage history, notifications of failure, usage history and status updates between the device and the service provider. Instead, this section relates to receiving an authentication request to validate a user request. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device that includes a request handler that receives activity requests from the service provider and the device. Lloyd does not teach this limitation because it is not concerned with a gateway device that includes a request handler that receives activity requests from the service provider and the device

The Examiner referenced col. 5, lines 38-40 as being relevant to a system including an appliance in a first network (Figure 1, workstation 128) and referenced col. 4, lines 15-21 as being relevant to a service provider in a second network (Figure 1, elements 110, 114 and 116). Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a system for securely providing services between a first site and a second site comprising an appliance linked in a first network at the first site

and a service provider linked to the appliance in a second network at the second site. Instead, these sections relate to a user requesting access to a network from a workstation connected to a network server access (NAS) device and the types of network elements that are attached to the network, wherein the network elements represent certain services that are available to users having access to the network. The teaching in this section is not analogous to the claimed limitation because there is no mention of a system including an appliance in a first network and a service provider in a second network. Lloyd does not teach this limitation because it is not concerned with a system for securely providing services between a first site and a second site comprising an appliance linked in a first network at the first site and a service provider linked to the appliance in a second network at the second site and securely managing the services between the at least one appliance and the service provider, wherein the services comprise exchanging status information, diagnostic information, usage history, notifications of failure, usage history and status updates between the device and the service provider. Instead, Lloyd is only interested in the creation of a single database that maintains accounting information user authentication information and authorization information to authorize user access to a computer network.

In addition, Lloyd does not disclose a system for securely providing remote monitoring and diagnostics as recited in claims 45 and 84 of the present patent application. Claims 45 and 84 also recite limitations similar to the above noted independent claims, but are set out in a remote monitoring and diagnostics embodiment.

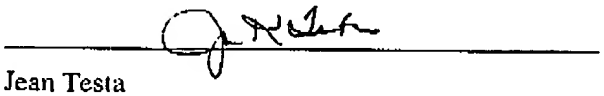
In view of the above-noted distinctions, Applicant submits that the claimed invention as recited in independent claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101 is patentably distinguishable over Lloyd. Accordingly, Applicant submits that Lloyd does not anticipate claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101.

Claims 2-9, 11-18, 20-25, 28-35, 37-44, 46-53, 55-61, 63-69, 71-75, 77-83, 85-91 and 93-99 depend directly or indirectly from now presumably allowable claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101, respectively, and thus are allowable by dependency. Accordingly, Applicant requests that the Examiner reconsider and remove the §102(e) rejection of claims 1-101 under Lloyd.

In view of the foregoing amendment and for the reasons set out above, Applicant requests that the Examiner reconsider this application and allow claims 1-101.

Should the Examiner believe that anything further is needed to place the application in even better condition for allowance, the Examiner is requested to contact the Applicant's undersigned representative at the telephone number below.

Respectfully submitted,



Jean Testa

Reg. No. 39,396

May 13 ,2005

General Electric Company
Building K1, Room 3A62
Schenectady, New York 12301
Telephone: (518) 387-5115